

262
AF \$



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

APPELLANTS: Turner et al. CONFIRMATION NO. 3107
SERIAL NO.: 10/007,899 GROUP ART UNIT: 2116
FILED: November 5, 2001 EXAMINER: Tse W. Chen
TITLE: "ARRANGEMENT FOR THE POWER SUPPLY FOR A
SECURITY DOMAIN OF A DEVICE"

MAIL STOP APPEAL BRIEF-PATENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANTS' MAIN BRIEF ON APPEAL

S I R:

In accordance with the provisions of 37 C.F.R. §41.37, Appellants herewith submit their main brief in support of the appeal of the above-referenced application.

REAL PARTY IN INTEREST:

The real party in interest is Francotyp-Postalia GmbH, a German corporation, as successor to Francotyp-Postalia AG & Co. KG, assignee of record for the application.

RELATED APPEALS AND INTERFERENCES:

There are no related appeals and no related interferences.

STATUS OF CLAIMS:

Claims 1-3 and 5-14 are at issue in the present appeal. All of these claims were finally rejected in the Office Action dated February 1, 2006. Claim 4 of the application is still pending, and was objected to in that Office Action, and was stated

to be allowable if rewritten in independent form. No other claims were or are present in the application.

STATUS OF AMENDMENTS:

No Amendment was filed subsequent to the Final Rejection.

SUMMARY OF CLAIMED SUBJECT MATTER:

Modern postage meter machines or other devices for franking postal items are equipped with a printer for printing the postage stamp on the postal matter, a controller for controlling the printing and the peripheral components of the postage meter machine, an accounting unit for debiting postage fees that are stored in non-volatile memories, and a unit for cryptographically securing the postage fee data. (p.1, l.16-20) Information that could be used by a postal counterfeiter, such as cryptographic keys and downloaded, electronically stored postage funds, are required by most governmental postal (tape is bad) contained in a substantially tamper-proof component, commonly known as a postal security device (PSD). If, as is common, the data are stored in a volatile memory, the PSD must be provided with a battery to provide back-up power in the event of a power loss to the PSD, or the postage meter containing the PSD. Because of the requirement to make the PSD tamper-proof, access to the back-up battery therein is extremely difficult, if not impossible. If frequent power outages occur so that the back-up battery in the PSD is frequently required to provide back-up power, this back-up battery becomes drained and must be replaced before the end of its normal lifetime. Since such replacement of the battery (or any component) in the PSD presents the aforementioned problems, there is a need to avoid overuse of the back-up battery in

the PSD so that it, or the PSD containing it, need be replaced only at the end of the normally expected lifetime of the back-up battery.

This is achieved by the electronic device set forth with claims on appeal that has a security region containing a first battery, which supplies power to security components in the security region, and which is connected to a first input of a battery switchover device, also located in the security region. A second battery is disposed in the device outside of the security region and is connected to a second input of the battery switchover device. A monitoring unit monitors voltage information relating at least to the second battery and activates the battery switchover device. (p4, l.9-15)

The provision of a battery compartment in a non-security region of the device housing in combination with a battery switchover device and a monitoring unit offers protection against incorrect polarization, oxidation of the battery contact posts and protection against non-insertion of a second battery in the implementation of a battery replacement. By taking over the supply of the power-consuming components, the second battery lengthens the service life of the first battery. Since battery replacement can be undertaken by a user of the device, the service life of the security module can be significantly increased without requiring the unit to be returned to the manufacturer. Protection against manipulation of the stored data is guaranteed because the provision of the battery compartment does not compromise the security region of the device housing. (p.4, l.18 - p.5, l. 19)

Figure 1 shows an arrangement for the power supply for a security domain of a device. The device, for example a mail processing unit, a postage meter machine or a computer, has a security region 10 and at least one non-security region 14. (p. 6, l.4-6) A first battery 134 in the security region ensures an emergency power

supply of components (not shown) given outage of the main power supply, a second battery 140 serves as an auxiliary power supply. (p.6, l.6-9) The first battery 134 — for example a 3 V lithium battery of the type — has a nominal voltage U_{BA} . The second battery 140 is replaceably arranged in the non-security region 140 and has a nominal voltage U_{BB} . (p.6, l.9-12) The two batteries are decoupled from one another via a battery switchover device 18 and are interconnected such that the higher battery voltage is present at the output thereof, whereby $U_B = U_{BB}$ if $U_{BA} < U_{BB}$, and $U_B = U_{BA}$ if $U_{BA} > U_{BB}$. (p.6, l.12-14) The output-side voltage U_B serves for the supply of the monitoring unit 21 and further components in the security region 10. For example, the second battery 140 is a lithium battery. (p.6, l.14-16) Via the line 189, its positive pole is connected to one of the two inputs of the battery switchover device 18. The first battery 134 has its positive pole 103 connected to the other of the two inputs of the battery switchover device 18. (p.6, l.17-20) With $U_{BB} = 3.6$ V, thus, the second battery has a somewhat higher voltage than the first battery 134 ($U_{BA} = 3$ V). The output of the battery switchover device 18 applies the battery voltage $U_B = U_{BB} - UV$ to components (not shown) in the security region 10. (p.6, l.20-23) The voltage UV represents drops at the diodes/switches. The first battery 134 is directly located in the security region 10 of the device, for example of a postage meter machine, that is not accessible to the user. At least a part of the security region 10 can be fashioned as a security module. (p.6, l.24 - p.7, l.2) Differing from conventional replaceable batteries used for this purpose, the first battery 134 can be firmly soldered on the security module and serves as emergency battery and can be relatively small and inexpensive. (p.7, l.2-5) The retention time given exclusive supply by this battery 134 can be on the order of one year; however,

the storage time of this battery 134 must be ≥ 10 years. This battery 134 can already be connected during the production process to the security module/component in need of battery voltage in order to enable the storage of information therein (initialization). (p.7, l.6-9)

In a first embodiment, a first series circuit of Schottky diodes 183, 184 and a second series circuit of Schottky diodes 185, 186 are respectively connected between the first and second inputs of the battery switchover device 18 and the output of the battery switchover device 18. The output of the battery switchover device 18 lies on a line 193. The voltage drop across one of the Schottky diodes of the battery switchover device 18 typically lies between 100 and 200 mV. Advantageously, the battery switchover device 18 can be a component of the security module. (p.7, l.10-16)

The respective center taps 187, 188 of the first and second series circuit of Schottky diodes of the battery switchover device 18 are connected to inputs of an analog-to-digital converter of a monitoring unit 21. The latter can likewise be a component of the security module. (p.7, l.17-20) The security module preferably has a module processor with the analog-to-digital converter, integrated therein, as explained in greater detail on the basis of Figure 4. (p.7, l.20-22) The comparator can compare an actual value thereto that is supplied to a second input of the comparator from the center tap 187. (p.7, l.22 - p.8, l.2)

Figure 2 shows an illustration of the power supply within a postal security device independently of the embodiment of the battery switchover device 18. (p.8, l. 9-10) (p.8, l.9-10) At its output side, the battery switchover device 18 (which itself is not shown in Fig. 2) supplies a battery voltage U_B of approximately 2.6 through 3.2

V. (p.8, l.10-12) A system voltage U_{S+} of approximately 3.3. V is present at the components of a first supply region and at a first input of a battery/system voltage switchover device 180. (p.8, l.12-14) The battery voltage U_B is present at the second input thereof. The output of the battery/system voltage switchover device 180 supplies a voltage to the components of a second supply region 1002, which include postal registers, the real-time clock, and a unit for monitoring the battery voltage and for monitoring ambient conditions (for example, temperature). (p.8, l.14-18) The components of the first supply region 1001 are the processor of the postal security module PSD, memories (flash and SRAM), an application specific circuit ASIC, and analog-to-digital converter and a unit that monitors the system voltage. (p.8, l.18-21) An electronic battery voltage monitoring unit taps a battery voltage either on the busbar 193, i.e. between the switches and the user, or separately for each battery between the battery and switches or — as shown in Figure 1 — preferably at the tap between the switches. (p.8, l.21 - p.9, l.1) The voltage monitoring circuit only has to be activated when the machine is operating. The need for a replacement of the second battery 140 is called to the attention of the user by suitable known means. As a result, the replacement intervals can be adapted to the actual capacity of the second batteries and the second batteries are utilized better. This can expediently ensue with a display unit of the device or signaling means. (p.9, l.1-6) If the user does not undertake a replacement despite these prompts, the user is ultimately caused to replace the battery due to a change in the operation of the device. If the display/signaling is ignored, the postage meter machine can exhibit a specific behavior, possibly following a delay period. For example, the processor of the PSD

can be programmed to block the device after a delay period when the required replacement of at least the second battery 140 is not performed. (p.9, I.6-11)

Figure 3 shows a perspective view of the postage meter machine from the front. At its upper side, the meter 2 has a user interface with a display unit 4 and a keyboard, with a signal opening 20 for signaling the statuses of the security module. (p.9, I.12-15) The security module is plugged onto the motherboard of the meter of the postage meter machine or of some other suitable device that is preferably fashioned as security housing. (p.9, I.15-17) The meter housing is designed such that the user can see the status display of the security module from the outside through the opening 20, whereby the opening 20 extends up to the user interface of the meter 2. (p.9, I.18-20) The display/signaling is directly controlled by the internal microprocessor (module processor) of the security module and thus cannot be manipulated from the outside. (p.9, I.20-22) The display is always active in the operating condition of the postage meter machine, so that the application of the system voltage U_{s+} to the module processor of the security module suffices for activating the display in order to be able to read the module status. (p.9, I.22 - p. 10, I.1) A security region (not shown) that is located inside the meter 2 under the keyboard 5 and is not accessible from the outside, contains the security module PSD and is separated from a non-security region by a sheet metal barrier. (p.10, I.1-4) A battery compartment that can be closed with a battery flap 16 arranged downstream at a sidewall of the meter 2 in the mail stream is provided in the non-security region. (p.10, I.4-6)

The second battery can be replaced by a technician and/or user without having to open that part of the postage meter machine that is specially postally

secured. The second battery therefore need not be dimensioned for the full service life of the machine, but the aforementioned problems with respect to the battery replacement nevertheless are avoided. (p.10, l.7-11) The second battery 140 thus is positioned at a location that can be easily reached by technicians and/or user, preferably in the externally accessible battery compartment. (p.10, l.11-13) Given outage of the system voltage, the components are supplied only by the second battery 140, controlled by the electronic switches or by the voltage amplitude in the case of diodes. (p.10, l.13-15) The first battery 134 is then purely as reserve for the time the second battery 140 is replaced or in case the latter is drained. In this arrangement, the first battery 134 therefore reaches approximately its maximum service life and need not be changed in the desire time span of approximately 12 years. (p.10, l.15-18)

GROUND OF REJECTION TO BE REVIEWED ON APPEAL:

The following issues are presented in the present appeal:

whether the subject matter of claims 1, 5-11 and 14 would have been obvious to a person of ordinary skill in the field of providing back-up power to a tamper-proof component, under the provisions of 35 U.S.C. §103(a), based on the teachings of PCT Application WO 99/48055 (Naclerio) in view of the teachings of United States Patent No. 5,650,974 (Yoshimura);

whether the subject matter of claims 2 and 3 would have been obvious to a person of ordinary skill in the field of providing back-up power to a tamper-proof component, under the provisions of 35 U.S.C. §103(a), based on the teachings of Naclerio and Yoshimura, further in view of the teachings of United States Patent No. 6,073,085 (Wiley et al.); and

whether the subject matter of claims 12 and 13 would have been obvious to a person of ordinary skill in the field of providing back-up power to a tamper-proof component, under the provisions of 35 U.S.C. §103(a), based on the teachings of Naclerio and Yoshimura, further in view of the teachings of United States Patent No. 5,128,552 (Fang et al.).

ARGUMENT:

Rejection of Claims 1, 5-11 and 14 Under 35 U.S.C. §103(a) Based on Naclerio and Yoshimura

The Naclerio reference discloses a tamper-resistant postal security device that addresses the same problem as the claims on appeal, namely extending the life of the internal back-up battery, but the solution disclosed in the Naclerio reference is based on a completely different concept (reducing the amount of data that must be backed up) compared to the subject matter of the claims on appeal (providing an additional back-up battery outside of the secured region). In general, it is the position of the Appellants that since the Naclerio reference already provides a solution to this problem, a person of ordinary skill in this technology would have no reason to modify the Naclerio reference in order to provide another solution to the problem that is already solved in the Naclerio reference, in a different manner. Since the Naclerio reference teaches a solution to extending the battery life of the internal battery by minimizing the amount of data that must be backed up, and thereby reducing the drain on the internal battery in the event that a back-up is necessary, a person of ordinary skill in this field would consider it superfluous to undertake the additional expense of providing another battery, outside of the security region. If the Naclerio circuit operates as intended, and if the statements therein are assumed to

be correct, the drain on the internal battery in the postal security device is already minimized, and therefore “extra” measures for the same purpose would be superfluous.

The same problem discussed above in the present brief, and discussed in Appellants’ specification, namely the difficulty associated with replacing the internal battery of a postal security device, is discussed at pages 1-3 of the Naclerio reference. As explained at page 4 of the Naclerio reference, at lines 5-17, the solution to that problem disclosed in the Naclerio reference is to provide the postal security device with a non-volatile memory, which does not depend on battery power, such as an EEPROM, and a non-volatile memory which does depend on battery power, such a static RAM. The sensitive data to be protected in the event of a power loss in the Naclerio reference is an encryption key. When normal power is available to the postal security device, a large RAM such as a dynamic RAM, is available to store the large amount of data that is decrypted using the encryption key. The memory in which this large amount of data is stored is not backed-up with the internal battery; only the much smaller memory in which the cryptographic key is stored is backed up. Therefore, the drain on the internal battery is significantly reduced if and when a power loss to the postal security device occurs, and the internal battery must be activated.

Therefore, the Naclerio reference, although seeking to solve the same problem as the subject matter of the claims on appeal, proceeds in a completely different direction, both conceptually and in terms of circuitry. The Naclerio reference teaches away from the use of another back-up battery outside of the security device, and instead makes use of a much smaller memory that is backed up

by the one and only back-up battery, namely the internal battery in the security device.

This problem is solved in a completely different manner by the subject matter of the claims on appeal by providing a second back-up battery that is located outside of the physical barrier that protects the security module, and therefore this second back-up battery can be easily replaced, as needed. It is this second back-up battery that is normally used as the back-up battery for the components in the security module if an outage of mains voltage occurs. Only if an outage of mains voltage occurs and the second back-up battery itself cannot provide the necessary voltage (due to the second back-up battery itself being drained, or at the end of its lifetime, or simply absent for some reason) does the first back-up battery in the security module become connected to the components in the security module, by the battery switchover device, so as to supply power to those components. Therefore, since it is normally the second back-up battery, outside of the security region, that is used in the case of power outage of the mains voltage, the lifetime of the first back-up battery in the security module is prolonged, so that the likelihood of only having to replace that first back-up battery at the end of its normal lifetime is increased. Therefore, even if power outages occur relatively often, it is the second back-up battery that is used in those circumstances, which is unproblematical because the second back-up battery can be easily replaced, unlike the first back-up battery in the security region.

In applying the disclosure of the Yoshimura patent against the subject matter of claim 1 as a basis for modifying the Naclerio system, the Examiner characterized the Yoshimura memory device as having a "security region" on the basis that

sensitive data stored in the memory device had to be backed-up in the event of a power loss. The explicit language of claim 1 makes clear that the term “security region” does not mean merely a region that requires electronic back-up, but is a region to which physical access is normally precluded, by means of a mechanical security barrier. The mechanical security barrier is of the type described in the Naclerio reference to preclude tampering. Moreover, the security region that contains the first battery is described at many locations in the present specification as being a postal security device (PSD). Such a postal security device, as described in the Naclerio reference is a device that is well-known to those of ordinary skill in the field of designing franking machines, and must have such a mechanical security barrier that is in compliance with the governmental regulations of the postal authority in the country in which it is used.

The mere electronic protection against erasure of data in the Yoshimura reference is not the same as such a mechanical security barrier as set forth in claim 1.

Moreover, both BAT1 and BAT2 in the Yoshimura reference on which the Examiner relied as corresponding to the first and second batteries of claim 1 of the present application, are disposed in the *same* region of the Yoshimura device. There is no difference regarding access to either of the BAT1 or BAT2; either of those batteries can be easily replaced without any difficulty, unlike the first battery in claim 1 of the present application.

The only alleged “link” between the Naclerio and Yoshimura references is that the Examiner contends that the Yoshimura reference has a “security region” as set forth in the claims, and as is present in the Naclerio reference. For the reasons

discussed above, the Yoshimura reference does not disclose or suggest a security region that is encompassed by a physical barrier, as is explicitly set forth in claim 1 and is the case in the Naclerio reference. Therefore, there is no basis whatsoever for a person of ordinary skill seeking to solve problems associated with backing up a component that does, in fact, have such a "security region" to consult the Yoshimura reference. Moreover, as noted above, even if such a person did consult the Yoshimura reference, for reasons unknown to the Appellants, a solution comparable to that set forth in claim 1 would not be apparent from that reference because the two batteries in the Yoshimura reference are in the *same* region of the Yoshimura device.

The Federal Circuit stated in *In re Lee* 227 F.3d 1338, 61 U.S.P.Q. 2d 1430 (Fed. Cir. 2002):

"The factual inquiry whether to combine references must be thorough and searching. ...It must be based on objective evidence of record. This precedent has been reinforced in myriad decisions, and cannot be dispensed with."

Similarly, quoting *C.R. Bard, Inc. v. M3 Systems, Inc.*, 157 F.3d 1340, 1352, 48 U.S.P.Q. 2d 1225, 1232 (Fed. Cir. 1998), the Federal Circuit in *Brown & Williamson Tobacco Court v. Philip Morris, Inc.*, 229 F.3d 1120, 1124-1125, 56 U.S.P.Q. 2d 1456, 1459 (Fed. Cir. 2000) stated:

[A] showing of a suggestion, teaching or motivation to combine the prior art references is an 'essential component of an obviousness holding'.

In *In re Dembiczak*, 175 F.3d 994,999, 50 U.S.P.Q. 2d 1614, 1617 (Fed. Cir. 1999) the Federal Circuit stated:

Our case law makes clear that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is

rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references.

Consistently, in *In re Rouffet*, 149 F.3d 1350, 1359, 47 U.S.P.Q. 2d 1453, 1459 (Fed. Cir. 1998), the Federal Circuit stated:

[E]ven when the level of skill in the art is high, the Board must identify specifically the principle, known to one of ordinary skill in the art, that suggests the claimed combination. In other words, the Board must explain the reasons one of ordinary skill in the art would have been motivated to select the references and to combine them to render the claimed invention obvious.

In *Winner International Royalty Corp. v. Wang*, 200 F.3d 1340, 1348-1349, 53 U.S.P.Q. 2d 1580, 1586 (Fed. Cir. 2000), the Federal Circuit stated:

Although a reference need not expressly teach that the disclosure contained therein should be combined with another, ... the showing of combinability, in whatever form, must nevertheless be clear and particular.

Lastly, in *Crown Operations International, Ltd. v. Solutia, Inc.*, 289 F.3d 1367, 1376, 62 U.S.P.Q. 2d 1917 (Fed. Cir. 2002), the Federal Circuit stated:

There must be a teaching or suggestion within the prior art, within the nature of the problem to be solved, or within the general knowledge of a person of ordinary skill in the field of the invention, to look to particular sources, to select particular elements, and to combine them as combined by the inventor.

Appellants respectfully submit the Examiner has not satisfied these rigorous evidentiary standards in substantiating the rejection of claim 1 under 35 U.S.C. §103(a) based on the teachings of Naclerio and Yoshimura.

Claims 5-11 and 14 add further structure to the non-obvious combination of independent claim 1, and are submitted to be patentable over the teachings of Naclerio and Yoshimura for the same reasons discussed above in connection with claim 1.

Rejection of Claims 2 and 3 Under 35 U.S.C. §103(a) based on Naclerio, Yoshimura and Wiley et al.

With regard to claims 2 and 3, the Examiner has acknowledged that Naclerio and Yoshimura do not expressly disclose the use of an analog-to-digital converter for converting voltage information into digital information and the details of the monitoring circuit. The Examiner relied on the Wiley et al. reference as disclosing an electronic unit 50 that includes a monitoring unit that comprises an analog-to-digital converter.

Appellants do not dispute that the Wiley et al. reference, by itself, provides this individual teaching, but Appellants submit there is no guidance, inducement or motivation in any of the Naclerio, Yoshimura or Wiley et al. references to modify a combination of Naclerio and Yoshimura in accordance with this isolating teachings of Wiley et al. Moreover, claims 2 and 3 depend from independent claim 1 and, as extensively discussed above, the Naclerio and Yoshimura reference fail to disclose or suggest the subject matter of claim 1.

Therefore, claims 2 and 3 would not have been obvious to a person of ordinary skill in the relevant technology under the provisions of 35 U.S.C. §103(a), based on the teachings of Naclerio, Yoshimura and Wiley et al.

Rejection of Claims 12 and 13 Under 35 U.S.C. §103(a) Based on Naclerio, Yoshimura and Fang et al.

The Examiner has acknowledged that the combination of Naclerio and Yoshimura does not disclose details of the processing operations set forth in claims 12 and 13, and the Examiner has relied on the Fang et al. reference as disclosing such details. Appellants acknowledge that the Fang et al. reference teaches evaluating voltage information for determining a need to replace a battery, however,

the Fang et al. reference provides no teachings whatsoever regarding the use of multiple batteries, and therefore Appellants do not agree with the Examiner's conclusion that the Fang et al. reference provides any teachings whatsoever to monitor voltage information to determine if and when an unperformed need exists to replace a *second* battery, in the context that the term "second battery" is used in independent claim 1, from which claim 12 depends. The same is true with regard to claim 13.

Therefore, Appellants respectfully submit that none of the Naclerio, Yoshimura or Fang et al. references provides any guidance, motivation or inducement to modify the Naclerio/Yoshimura combination in order to arrive at the subject matter of either of claims 12 or 13.

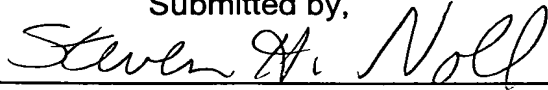
Moreover, for the reasons discussed extensively above, Appellants do not agree that the Naclerio/Yoshimura combination discloses or suggests the combination of independent claim 1, from which claims 12 and 13 depend, and therefore even if the Naclerio/Yoshimura combination were modified in accordance with the teachings of Fang et al., for reasons unknown to the Appellants, the combinations of claims 12 and 13 still would not result.

CONCLUSION:

For the above reasons, Appellants respectfully submit the Examiner is in error in law and in fact in rejecting claims 1-3 and 5-14 on appeal. Reversal of those rejections is proper, and the same is respectfully requested.

This Appeal Brief is accompanied by a check for the requisite fee in the amount of \$500.00.

Submitted by,

 (Reg. 28,982)

SCHIFF, HARDIN LLP

CUSTOMER NO. 26574

Patent Department

6600 Sears Tower

233 South Wacker Drive

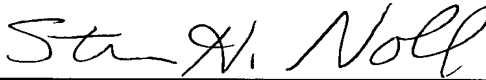
Chicago, Illinois 60606

Telephone: 312/258-5790

Attorneys for Appellants.

CERTIFICATE OF MAILING

I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on June 22, 2006.



STEVEN H. NOLL

CLAIMS APPENDIX

1. An electronic device comprising:
 - a security region containing a plurality of security components, said security region being surrounded by a mechanical security barrier to normally preclude physical access to said security components;
 - a power source adapted for connection to a mains voltage for normally supplying power to said security components;
 - a first battery disposed in said security region with physical access to said first battery also being normally precluded in said security barrier;
 - a second battery disposed outside of said security region for supplying power to said security components upon an outage of said mains voltage;
 - a battery switchover device having a first input connected to said first battery and a second input connected to said second battery for switching power supply to said security components from said second battery to said first battery only if power from said second battery is absent; and
 - a monitoring unit disposed in said security region and connected to said battery switchover device for evaluating voltage information associated with at least one of a voltage of said first battery and a voltage of said second battery.
2. An electronic device as claimed in claim 1 wherein said monitoring unit comprises an analog-to-digital converter for converting said voltage information into digital information.
3. An electronic device as claimed in claim 2 wherein said monitoring unit comprises a processor supplied with said digital information for evaluating said

digital information to generate a signal indicating a supply status representative of said voltage information, and an externally visible indicator connected to said processor for receiving said status signal therefrom and for displaying a visual indication of said supply status.

5. An electronic device as claimed in claim 1 wherein said battery switchover device has an output connected to said security components for supplying power thereto via said battery switchover device from one of said first battery and said second battery, and wherein said device further comprises, in said security region, decoupling elements at said output.

6. An electronic device as claimed in claim 5 wherein said decoupling elements are selected from the group consisting of diodes and controlled electronic switches.

7. An electronic device as claimed in claim 1 further comprising a security module containing said monitoring unit and said security components and protected by said mechanical security barrier.

8. An electronic device as claimed in claim 7 wherein said security module further comprises said battery switchover device.

9. An electronic device as claimed in claim 1 further comprising a battery compartment for said second battery, closeable with a battery compartment cover.

10. An electronic device as claimed in claim 9 having a housing containing said security region and said battery compartment, and having a sidewall in which said battery compartment cover is disposed.

11. An electronic device as claimed in claim 9 having a housing containing said security region and said battery compartment, and having a base in which said battery compartment cover is disposed.

12. An electronic device as claimed in claim 1 further comprising a plurality of operating components, and wherein said monitoring unit includes a processor for evaluating said voltage information, and wherein said processor is connected to at least one of said operating components and alters operation of said at least one of said operating components if said voltage information indicates an unperformed need to replace said second battery.

13. An electronic device as claimed in claim 12 wherein said processor prevents operation of said at least one operating component after a predetermined delay if said voltage information indicates an unperformed need to replace said second battery.

14. An electronic device as claimed in claim 7 wherein said security module is a postal security device.

EVIDENCE APPENDIX

Exhibit A: Drawing sheet with Figs. 1, 2 and 3 -- part of application as originally filed on November 5, 2001.

Exhibit B: PCT Application WO 99/48055 (Naclerio) -- cited in Final Rejection dated February 1, 2006.

Exhibit C: United States Patent No. 5,650,974 (Yoshimura) -- cited in Final Rejection dated February 1, 2006.

Exhibit D: United States Patent No. 6,073,085 (Wiley et al.) -- cited in Final Rejection dated February 1, 2006.

Exhibit E: United States Patent No. 5,128,552 (Fang et al.) cited in Final Rejection dated February 1, 2006.

RELATED PROCEEDINGS APPENDIX

None.

CH1\ 4607098.1

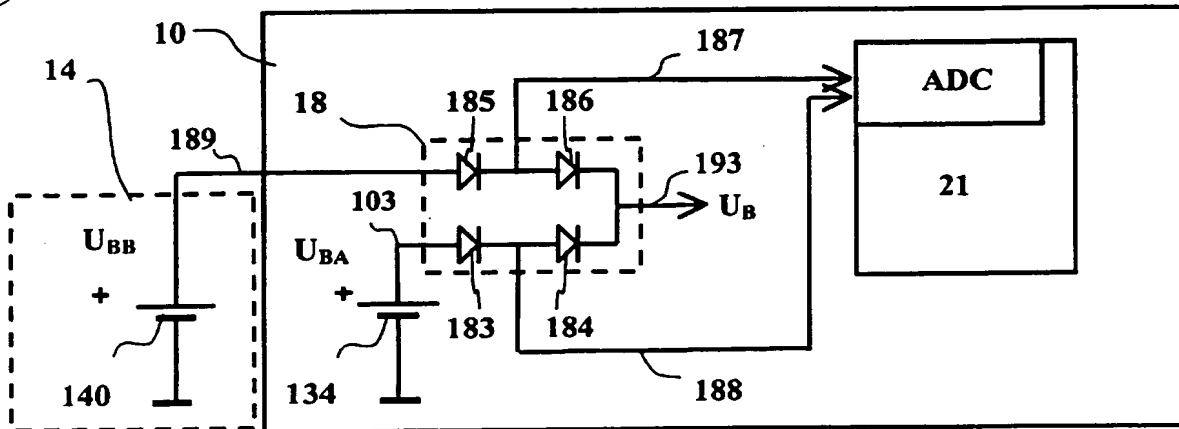


Fig. 1

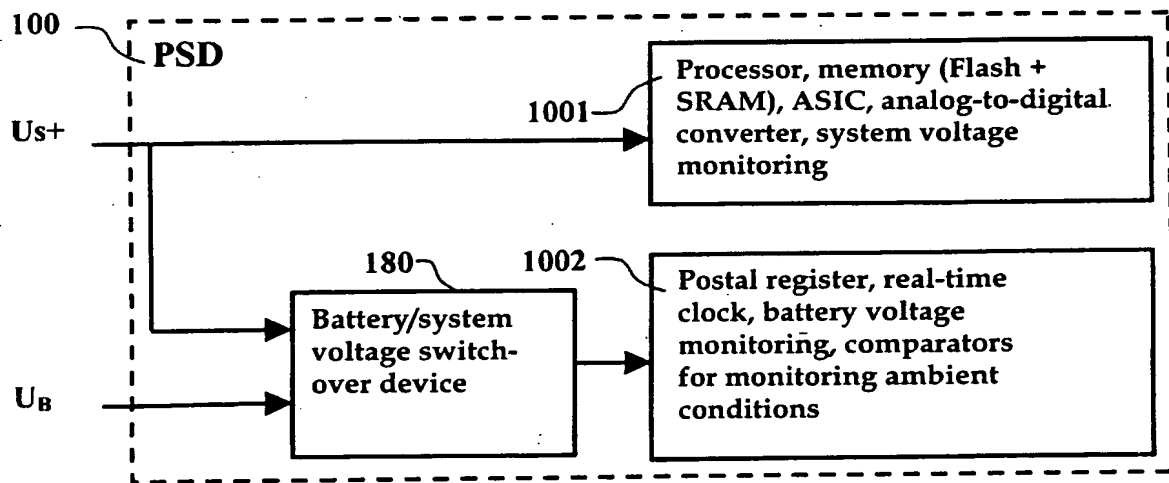


Fig. 2

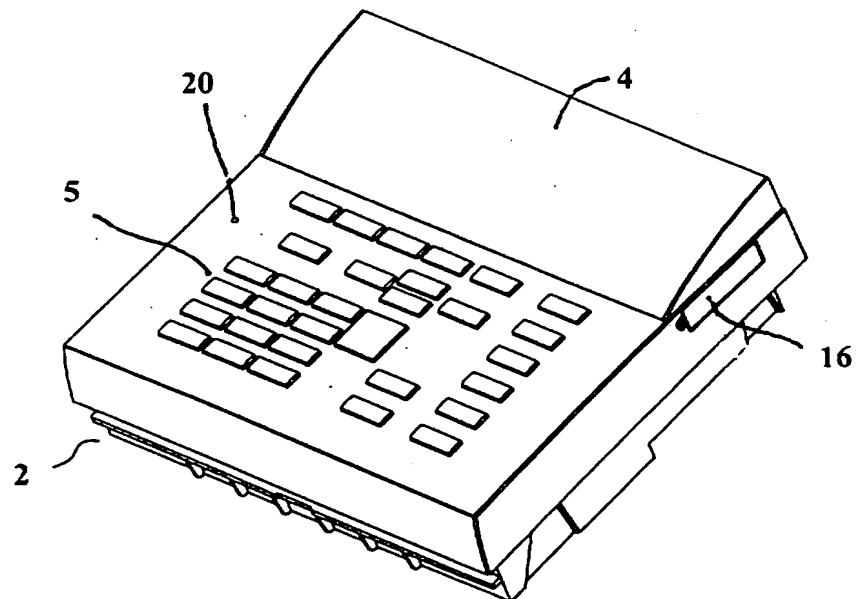


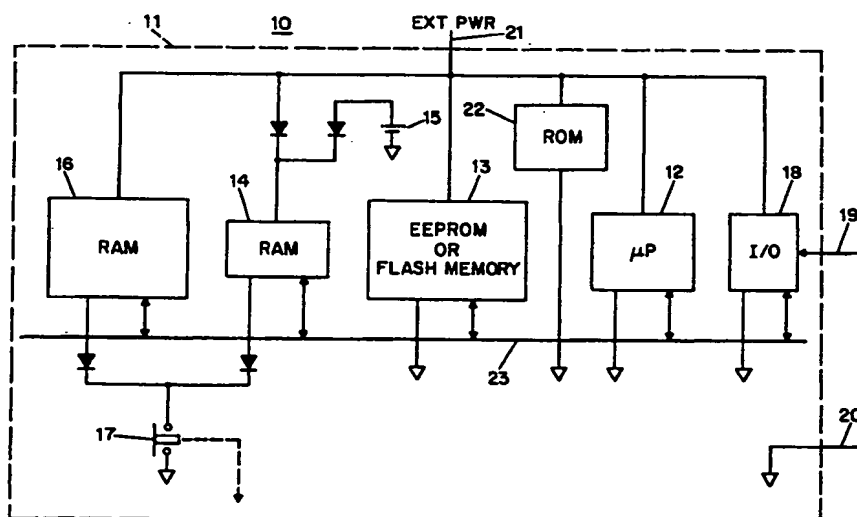
Fig. 3



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G07B 17/04	A1	(11) International Publication Number: WO 99/48055 (43) International Publication Date: 23 September 1999 (23.09.99)
(21) International Application Number: PCT/US99/05891 (22) International Filing Date: 18 March 1999 (18.03.99) (30) Priority Data: 60/078,489 18 March 1998 (18.03.98) US (71) Applicant (for all designated States except US): ASCOM HASLER MAILING SYSTEMS INC. [US/US]; 19 Forest Parkway, Shelton, CT 06484-6140 (US). (72) Inventor; and (75) Inventor/Applicant (for US only): NACLERIO, Edward, J. [US/US]; 49 Scenic Road, Madison, CT 06443 (US). (74) Agents: OPPEDAHN, Carl et al.; Oppedahl & Larson, P.O. Box 5270, Frisco, CO 80443-5270 (US).	(81) Designated States: CA, JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report.</i>	

(54) Title: TAMPER RESISTANT POSTAL SECURITY DEVICE WITH LONG BATTERY LIFE



(57) Abstract

In accordance with the invention, a postal security device (PSD) (10) contains a non-volatile memory (13) which does not depend on battery power such as an EEPROM (13), and contains a nonvolatile memory (14, 16) which does depend on battery power, such as a static RAM. The PSD (10) also contains an encryption engine (12, 14, 22). An encryption key is developed and is stored in the static RAM (14), which is sized to be only large enough to contain the encryption key. A large body of data, too large to fit in the static RAM, is encrypted by means of the encryption engine (12, 14, 22) and with reference to the encryption key, and is stored in the EEPROM (13). This body of data typically includes cryptographic keys and sensitive bit-images. When the PSD is powered, a large RAM (typically a dynamic RAM) (16) is available to receive the large body of data, decrypted using the encryption key. A tamper switch (17) cuts power to both RAMs (14, 16) in the event of tampering.

EXHIBIT B

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon	KR	Republic of Korea	PL	Poland		
CN	China	KZ	Kazakhstan	PT	Portugal		
CU	Cuba	LC	Saint Lucia	RO	Romania		
CZ	Czech Republic	LI	Liechtenstein	RU	Russian Federation		
DE	Germany	LK	Sri Lanka	SD	Sudan		
DK	Denmark	LR	Liberia	SE	Sweden		
EE	Estonia			SG	Singapore		

TAMPER RESISTANT POSTAL SECURITY DEVICE WITH LONG BATTERY LIFE

The invention relates generally to postage meters (franking machines), and relates particularly to systems in which postage value is stored in a postal security device (PSD) so as to be protected against undetected tampering. The application claims priority from US application
5 no. 60/078,489, filed March 18, 1998, which application is incorporated herein by reference to the extent permitted by the designated and elected States hereto.

Background

In recent years it has been proposed to print postal indicia by means of conventional nonsecure printers such as laser printers, ink-jet printers, and thermal transfer printers. Such
10 printers are termed "nonsecure" because the printer itself is not in a secure housing and because the communications channel linking the printer to other apparatus is nonsecure. Under such a proposal, the question naturally arises what would prevent a user from printing the same postal indicium repeatedly, thereby printing postal indicia for which no money has been paid to the post office. The proposed anti-fraud measure is to store information within
15 the indicia which would permit detecting fraud. The indicium would include not only human-readable text such as a date and a postage amount, but would also include machine-readable information, for example by means of a two-dimensional bar code. The machine-readable information would be cryptographically signed, and would include within it some information intended to make fraud more difficult. The information would typically include
20 an identification of the postage meter license (granted by the meter manufacturer or by the postal authorities, depending on the country), an indication of the number of mail pieces franked, the postage amount, a postal security device identifier about which more will be said later, the date and time, and a zip code or post code of the mail piece addressee.

The typical apparatus for printing such "encrypted indicia" postage includes what is called a
25 postal security device or PSD. The PSD has a secure housing, and within the secure housing are the accounting registers as well as a cryptographic engine. The engine permits cryptographic authentication and signing for communication with an external device such as

the computer of the meter manufacturer or of the post office. The engine also permits creation of postal indicia which contain specified information and which are cryptographically signed. The PSD may well be physically small as compared to traditional postage meters. The PSD may be the size of a PCMCIA card or the size of a smart card.

- 5 Within the PSD the memory must be protected against inadvertent damage due to malfunction of the processor of the PSD, for example as set forth in US Pat. No. 5668973, *Protection system for critical memory information* owned by the same assignee as the assignee of the present application. The PSD must handle power failure in a graceful fashion, for example as set forth in US Pat. No. 5712542, *Postage meter with improved handling of*
10 *power failure*, also owned by the same assignee as the assignee of the present application.

- To reduce smudging, the printer may preferably be that described in PCT publication no. 97-46389, *Printing apparatus*, also owned by the same assignee as the assignee of the present application. While it has been proposed that the PSD contain a real-time clock which is keeping time continuously, desirably this requirement may be avoided as described in PCT
15 publication no. 98-08325, *Printing postage with cryptographic clocking security*, also owned by the same assignee as the assignee of the present application. PSDs can form part of a network with multiple printers as described in PCT publication no. 98-13790, *Proof of postage digital franking*, also owned by the same assignee as the assignee of the present application.

- 20 The postal authorities face the question how the PSD can be protected from tampering. For example, the entire system of PSDs depends on the use of cryptographic keys. The keys are used for authenticating communications between the PSD and the manufacturer's system or the postal authority's system. Such communications are used to set up and maintain the PSDs, and are used to refill or "reset" the PSDs to reflect the ability to print more postage.
25 The keys are also used to cryptographically "sign" information printed in the postal indicia. If the cryptographic keys were compromised, a user might be able to defraud the post office or the PSD manufacturer or both.

Many approaches have been proposed for protection of such cryptographic keys from compromise. The usual approach is to place the cryptographic keys in a RAM (random access memory) of a type which keeps its contents only so long as the RAM receives power from a battery. The secure housing of the PSD is designed to include a tamper switch, so that if the secure housing is tampered with, the switch opens. The switch interrupts power to the RAM (and, in particular, interrupts battery power to the RAM) and its contents are lost. In this way the information in the RAM (for example, the cryptographic keys) is protected from tampering. Another proposed approach is to employ commercial memory chips (such as the Dallas Semiconductor DS1283 and Benchmarq bq3283) offer a pin on the package which will clear the memory based on a predetermined input voltage level. The tamper switch is set up to apply the predetermined voltage upon detection of tampering.

Many approaches have also been proposed for detection of the tampering. In EP 820 041, for example, it is suggested that the secure housing of an old-style mechanical or electromechanical postage meter be set up to contain an air pressure that is distinctively higher than or lower than normal atmospheric pressure. If the secure housing is violated, the pressure within the secure housing changes to match the ambient pressure. A sensor within the housing detects the pressure change and thus the violation. The sensor disables further function of the postage meter.

The approach of cutting power to a volatile memory such as the RAM discussed above has a drawback in that during periods of power-down, the RAM depends on an internal battery to avoid loss of the information in the RAM. Depending on the requirements of the postal authority, and on design decisions made by the PSD manufacturer, the quantity of data requiring protection may be quite large. The data to be protected may include cryptographic keys used for PSD configuration, keys used for remote resetting (refilling), keys used for signing postal indicia, and keys used for the management of the other keys. In addition it may be desired to protect the bit-images used to generate the human-readable portion of the printed indicia. A RAM big enough to hold all of these important items of data will also draw a non-negligible current from the internal battery. This may lead to a limited and commercially unacceptable battery life.

It would thus be desirable to have a PSD design which protects the many important items of data stored within, and yet which does not draw very much battery power and so permits a commercially acceptable battery life.

Summary of the invention

5 In accordance with the invention, a postal security device (PSD) contains a nonvolatile memory which does not depend on battery power, such as an EEPROM, and contains a nonvolatile memory which does depend on battery power, such as a static RAM. The PSD also contains an encryption engine. An encryption key is developed and is stored in the static RAM, which is sized to be only large enough to contain the encryption key. A large body of
10 data, too large to fit in the static RAM, is encrypted by means of the encryption engine and with reference to the encryption key, and is stored in the EEPROM. This body of data typically includes cryptographic keys and sensitive bit-images. When the PSD is powered, a large RAM (typically a dynamic RAM) is available to receive the large body of data, decrypted using the encryption key. A tamper switch cuts power to both RAMs in the event
15 of tampering. In this way, the battery power required to maintain the PSD during power-off periods is minimal, and yet the large body of data will be inaccessible in the event of tampering.

Description of the drawing

The invention will be described with respect to a drawing, of which:

20 Fig. 1 is a schematic functional block diagram of a system according to the invention.

Detailed description

Fig. 1 shows a postal security device (PSD) in accordance with the invention. The PSD has a microprocessor 12 which communicates on a bus 22 with an input/output (I/O) device 18, a memory which does not require battery backup 13 which may be for example an EEPROM or

flash memory, a relatively small RAM 14, a ROM 22, and a larger RAM 16. The I/O device 18 communicates with external apparatus by means of communications channel 19 which may be a serial asynchronous data line. External power 21 and ground 20 are also defined. The larger RAM 16, and most of the other active components, receive external power. The smaller RAM 14 is additionally able to receive power from a backup battery 15, preferably a lithium cell with a very long (e.g. ten year) life. A tamper switch 17 is provided which, when triggered, can cut power to both the small RAM 14 and the large RAM 16.

A large body of data is assumed to require protection from a tampering user. The EEPROM is selected to be large enough to hold this body of data after it has been encrypted. When power is applied and the system is stable, the body of data (or selected portions thereof) is decrypted and transferred to RAM 16. This decryption is performed by the microprocessor 12 executing a decryption routine stored in the ROM 22, and the decryption is done with respect to a decryption key in the RAM 14. Alternatively the decryption may be performed by an optional engine omitted for clarity in Fig. 1. The decrypted data in RAM 16 are used as needed for the ordinary functions of the PSD, which include communicating via the communications channel 19 with a user computer, with a manufacturer's system, or with a postal authority system, and can include generating postal indicia which are to be printed by means of a printer.

When external power 21 is cut off, or when the PSD undergoes a normal power-down routine, the information in the RAM 16 is lost. In contrast, the information in the RAM 14 is preserved even when external power 21 is lost, because of battery 15.

During normal operation the body of data that requires protection from a tampering user (or some portion of it) may be located "in the clear", that is, unencrypted, in the RAM 16. In the event that this data has changed, it may be necessary to encrypt the data and to store it again in the memory 13. This encryption is performed by the processor 12 executing encryption software in the ROM 22, or may optionally be performed by an encryption engine omitted for clarity in Fig. 1.

The power-down condition for the PSD 10 assumes that no power is present at line 21. In that event, the only powered device is RAM 14. RAM 14 was purposefully selected to be large enough to hold the encryption key but not much larger, and in any event is smaller than the large body of data that is understood to require protection from a tampering user. Because
5 of the limited size of the RAM 14, it does not draw as much current from the battery 15 as would be drawn by a larger RAM such as RAM 16. Thus, the battery life is optimized, especially as compared with the shorter battery life that would result if the large body of data were all in battery-backed-up RAM.

Tampering may happen during a time when external power 21 is present. At a minimum, the
10 tamper switch should cut power to the RAM 14. (Or, alternatively, the tamper switch should apply to RAM 14 the predetermined voltage that clears the RAM.) Preferably the tamper switch will also cut power to the RAM 16 (or clear the RAM 16), for the reason that some of the body of sensitive data may be present "in the clear" in the RAM 16, and should not fall into the hands of the tampering user. Alternatively the tamper switch might trigger an
15 interrupt in the processor 12 which would cause the processor 12 to clear the sensitive portions of the RAM 16.

Tampering may also happen during a time when external power 21 is absent. In such a case, the RAM 16 is already, by definition, empty, as it is unpowered. The tamper switch causes the RAM 14 to be cleared. If the tampering user extracts the contents of the memory 13, this
20 is of little significance, because the contents are useless unless decrypted with the assistance of the key that is no longer present in the RAM 14. If the PSD 10 is powered up again after the tampering, the decryption routine will not work because the key of RAM 14 is gone. In addition, desirably the processor 12, under program control, will note the fact that RAM 14 is empty and will immediately attempt to send a message via communications channel 19 to the
25 manufacturer or to the postal authority.

Those skilled in the art will readily appreciate that design considerations may prompt the use of electrical components in addition to or instead of those shown in Fig. 1, none of which depart in any way from the invention. For example, dedicated cryptographic chips may be

employed which take some of the computational burden from the microprocessor. As another example, the particular way in which the tamper switch cuts power to the RAM may be varied, and the particular type of tamper switch may be selected among several types, all without departing in any way from the invention. Those skilled in the art will indeed have no
5 difficulty devising obvious variations and improvements to the invention, all of which are intended to be encompassed by the claims that follow.

Claims

1. A postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type requiring electrical power to maintain the contents thereof, said postal security device also comprising a battery powering the second memory and a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine, said body of data encrypted by the cryptographic engine with respect to the encryption key.

2. A method for use with a postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type that requires electric power to maintain its contents, said postal security device also comprising a battery powering the second memory and a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine; the method comprising the steps of:

storing the encryption key within the second memory;

encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory; and

in the event of tampering, removing power from the second memory.

- 5 3. A method for use with a postal security device comprising a secure housing, and within
the secure housing a body of data having a size, said postal security device also having within
the secure housing means for generating print data for printing of postage indicia, said
generating of said print data relying in part on the body of data, said postal security device
also having within the secure housing a first memory sized to accommodate the body of data,
10 said first memory of a type not requiring electrical power to maintain the contents thereof,
said postal security device also having within the secure housing a second memory not large
enough to accommodate the body of data, said second memory of a type that clears its
contents upon a predetermined electrical condition, said postal security device also
comprising a tamper switch mechanically coupled with the secure housing so that upon
15 tampering with the secure housing the second memory has said predetermined electrical
condition, said postal security device further comprising an encryption key stored within said
second memory, said postal security device further comprising a cryptographic engine; the
method comprising the steps of:

storing the encryption key within the second memory;

- 20 encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory; and

in the event of tampering, causing said predetermined electrical condition.

1/1

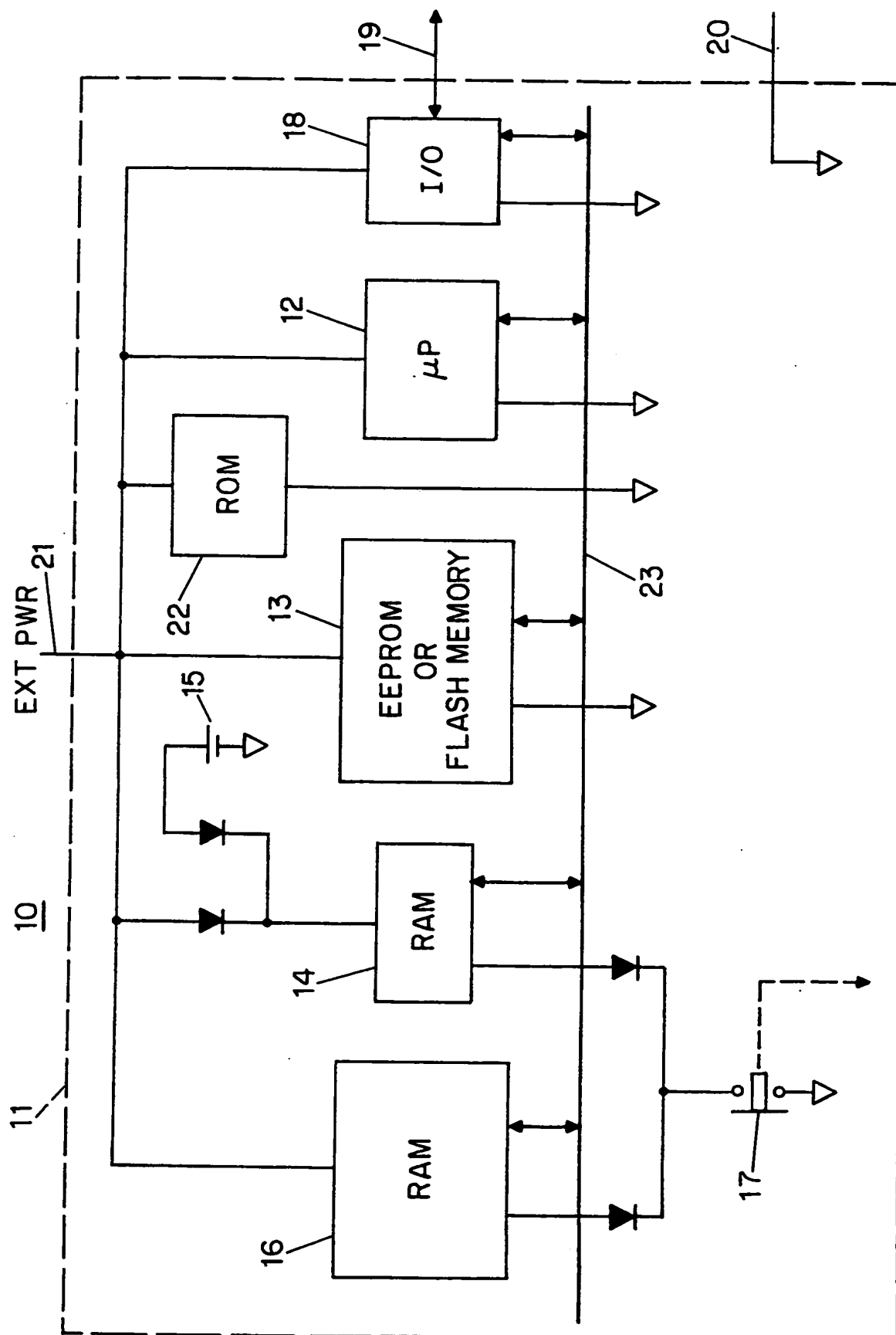


FIG. 1

SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

National application No.
PCT/US99/05891

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G07B 17/04

US CL : 705/405

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/3, 4, 23, 25; 705/401, 405, 410

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NoneElectronic data base consulted during the international search (name of data base and, where practicable, search terms used)
None

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,575,621 A (DREIFUS) 11 March 1986, see abstract.	1-3
A	US 4,882,752 A (LINDMAN et al) 21 November 1989, see abstract.	1-3
A	US 5,097,253 A (ESCHBACH et al 17 March 1992, see abstract.	1-3
A	US 5,249,227 A (BERGUM et al) 28 September 1993, see abstract.	1-3

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be of particular relevance	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
E earlier document published on or after the international filing date	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*A* document member of the same patent family
O document referring to an oral disclosure, use, exhibition or other means	
P document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

15 MAY 1999

Date of mailing of the international search report

28 MAY 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

EDWARD R COSIMANO

Telephone No. (703) 308-3800

Form PCT/ISA/210 (second sheet) (July 1992) *